



DORON YONISY

Risk Management | Chief Risk Officer

עמותת דורון (לדוגמה) ע.ר.

יום עיון בנושא

הגנת הפרטיות

דצמבר 2020

חוק הגנת הפרטיות התשמ"א - 1981

חוק הגנת הפרטיות עוסק בהגנה על שלמות המידע או הגנה על המידע מפני חשיפה, שימוש או העתקה ללא רשות.
החוק קובע כי לא ישתמש אדם במידע הקיים במאגר המידע אשר ברשותו אלא למטרות שלשמן הוקם המאגר.

הגדרת מושגים בהתאם לחוק הגנת הפרטיות

- ❖ **"מאגר מידע"** - אוסף של נתוני מידע, המוחזק באמצעי מגנטי או אופטי (למעט אוסף לשימוש אישי שאינו עסקי או מידע הכולל רק שם, כתובת ודרכי התקשרות).
- ❖ **"מידע"** - מוגדר כנתונים על אישיותו של אדם, מצב בריאותו, מצבו הכלכלי, הכשרה מקצועית, דעותיו ואמונתו.
- ❖ **"מידע רגיש"** - הינו כול "מידע" לרבות מידע ששר המשפטים קבע בצו שהוא מידע רגיש.
- ❖ **"רשם"** - הינו רשם מאגרי המידע.
- ❖ **"מנהל מאגר מידע"** - מנהל פעיל של גוף שבבעלותו מאגר מידע או באחזקתו מאגר מידע.
- ❖ **"מחזיק במאגר מידע"** - מי שמצוי ברשותו מאגר מידע דרך קבע והוא רשאי לעשות בו שימוש (לרבות גילוי, העברה או מסירה).
- ❖ **"שימוש"** - לרבות גילוי, העברה ומסירה.
- ❖ **"אבטחת מידע"** - הגנה על שלמות המידע או הגנה על המידע מפני חשיפה, שימוש או העתקה והכל ללא רשות כדין.

הרשות להגנת הפרטיות

הרשות להגנת הפרטיות היא רשות אכיפה ורגולציה שתפקידה להגן על פרטיות המידע האישי במרחב הדיגיטלי בארגונים מסחריים, בעסקים, במשרדי הממשלה, בגופים ציבוריים וברשויות ציבוריות. הרשות פועלת על ידי חוקרים ומפקחים מוסמכים מטעם הרשות, במטרה לאתר הפרות של חוק הגנת הפרטיות, להגביר את מודעות המשק להוראות החוק, לאתר כשלים ענפיים הדורשים התערבות ולקבל תמונת מצב מגזרית לגבי עמידה בהוראות החוק. הפנמת הגופים הרלוונטיים במשק את ערך הפרטיות ואמונו הגדול של הציבור בהם בעקבות כך, תורמים לפיתוח הצמיחה הכלכלית במשק ועל כן חשובים לאין שיעור.

הרשות מוסמכת לפעול ב- 3 תחומים עיקריים:

- ▶ אכיפה מנהלית – הטלת קנסות כספיים בפרק זמן הסמוך לאיתור ההפרה של החוק מבלי הצורך לערב את הרשות השופטת
- ▶ אכיפה פלילית – הרשות מוסמכת לחקור חקירות פליליות ולהעבירן לפרקליטות המדינה על מנת להגיש כתבי אישום
- ▶ פיקוח רוחב - הגופים המנהלים או המחזיקים מאגרי מידע נדרשים להשיב על שאלוני ביקורת של הרשות.

סוגי מאגרי מידע

בחודש מאי 2017 פורסמו תקנות אבטחת מידע, אשר נכנסו לתוקף בחודש מאי 2018, ואשר מגדירות לראשונה את סוגי מאגרי המידע הקיימים, כדלהלן:

- ▶ "מאגרים שחלה עליהם רמת אבטחה גבוהה"
- ▶ "מאגרים שחלה עליהם רמת אבטחה בינונית"
- ▶ "מאגרים שחלה עליהם רמת אבטחה בסיסית".
- ▶ "מאגר המנוהל בידי יחיד"
- ▶ "מאגר ביומטרי"



מאגר מידע ברמת אבטחה גבוהה

מאגר מידע שחלה עליו רמת אבטחה גבוהה הינו מאגר הכולל מידע על 100,000 איש ומעלה
או שמספר בעלי ההרשאה בו עולה על 100 ואשר:

❖ מאגר שמטרתו העיקרית לאסוף מידע לצורך מסירתו לאחר כדרך עיסוק, לרבות שירותי
דיוור ישיר

❖ מאגר מידע שבעליו הוא גוף ציבורי

❖ מאגר מידע הכולל מידע שהוא אחד מאלה:

- מידע על צנעת חייו האישיים של אדם
- מידע רפואי או מידע על מצבו הנפשי של האדם
- מידע גנטי
- מידע אודות עברו הפלילי של אדם
- מידע על נכסים, חובות, התחייבויות, מצב כלכלי
- הרגלי צריכה של אדם היכולים ללמד על צנעת חיו, מצבו הבריאותי, מצבו הכלכלי



מאגר מידע ברמת אבטחה בינונית

מאגר מידע שחלה עליו רמת אבטחה בינונית הינו מאגר הכולל את כל המאפיינים של מאגר מידע "ברמת אבטחה גבוהה". השוני היחידי נעוץ בכך שמספר האנשים שיש עליהם מידע הינו פחות מ- 100,000 ומספר העובדים העלי הרשאת כניסה למידע הינו פחות מ- 100 עובדים.

מאגר מידע ברמת אבטחה בסיסית

מאגר מידע שחלה עליו רמת אבטחה בסיסית הינו מאגר הכולל מידע על מועסקים או ספקים המשמש לניהול עסק בלבד, אינו כולל מידע בדבר צנעת הפרט, מידע גנטי, מידע אודות השקפות פוליטיות ודתיות ומידע ביומטרי ושמספר בעלי הרשאה אינו עולה על 10 עובדים.

מאגר המנוהל בידי יחיד

מאגר מידע שמנוהל על ידי יחיד או תאגיד בבעלות יחיד ואשר רק היחיד או לכל היותר שני בעלי הרשאה נוספים רשאים לעשות בו שימוש. (בנוסף מאגר זה אינו כולל מידע על יותר מ- 10,000 אנשים ואינו מיועד לדיוור ישיר)



פעולות שיש לעשות

- ❖ רישום המאגר
- ❖ בקרה ותיעוד גישה
- ❖ מינוי ממונה אבטחה
- ❖ אבטחה פיזית
- ❖ מסמך הגדרות המאגר
- ❖ אבטחת תקשורת
- ❖ מיפוי מערכות המאגר
- ❖ התקנים ניידים
- ❖ נוהל אבטחה
- ❖ ביקורות תקופתיות
- ❖ ניהול הרשאות כ"א

דוגמאות

שאלות...



רישום המאגר

בהתאם לסעיף 8ג בחוק להגנת הפרטיות תשמ"א נדרשת העמותה ברישום מאגר המידע אצל רשם מאגרי המידע שבמשרד המשפטים.

ככלל כל מאגר העומד באחד מהקריטריונים הבאים חייב ברישום :

חלק מפרטי טופס לרישום המאגר כולל מידע בדבר :

- ❖ זהות בעל המאגר, המחזיק במאגר ומנהל המאגר בפועל
- ❖ מטרת הקמת המאגר מיידע ולמה הוא קיים
- ❖ סוגי המידע שיהיו קיימים במאגר
- ❖ פרטים על העברת מידע מחוץ לגבולות המדינה
- ❖ פרטים על קבלת מידע מגוף ציבורי – שם בגוף ומהות המיידע שנמסר



מינוי ממונה אבטחה

אבטחה היא הגנה על שלמות המידע וכן הגנה מפני חשיפה, שימוש או העתקה ללא רשות. אבטחת המידע צריכה להיות באחריות בעל המאגר, מחזיק המאגר ומנהל המאגר.

בהתאם לסעיף 3 בתקנות הגנת הפרטיות (אבטחת מידע) :

”חלה חובה למנות ממונה על אבטחת מידע... ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או מנהל פעיל של בעל המאגר...או לנושא משרה בכירה הכפוף ישירות למנהל המאגר”

כמו כן, במסגרת רישום מאגר המידע נידרש בעל המאגר להודיע לרשם המאגרים במשרד המשפטים את שמו וזהותו של **”הממונה על אבטחת המידע”**.



מסמך הגדרות המאגר

בהתאם לסעיף 2 (א) בתקנות הגנת הפרטיות (אבטחת מידע): "בעל מאגר מידע" במסמך

הגדרת המאגר" את כל העניינים האלה לפחות :

1. תיאור כללי של פעולות האיסוף והשימוש שלו ;
2. תיאור מטרות השימוש במידע ;
3. סוגי המידע השונים הכלולים במאגר המידע ;
4. פרטים על העברות מאגר מידע או חלק מהותי ממנה מחוץ לגבולות המדינה ;
5. פירוט על מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר ;
6. פעולות עיבוד מידע באמצעות מחזיק מאגר ;
7. הסיכונים העיקריים של פגיעה באבטחת המידע ואיך מתמודדים איתם ;
8. שמם של מנהל מאגר המידע, מחזיק המאגר והממונה על אבטחת המאגר.

בהתאם לסעיף 2(ב) כאשר מתרחש שינוי משמעותי באחד מהסעיפים הנ"ל, או בעת שינויים

טכנולוגיים, על בעל המאגר לשנות את "מסמך הגדרות המאגר" בהתאם לשינויים שהתרחשו.



מיפוי מערכות המאגר

בהתאם לסעיף 5א בתקנות הגנת הפרטיות, על בעל מאגר המידע **לגבש מסמך הממפה את מערכות המידע**, מבנה המערכת ופרטי המצאי המרכיבים את מערכת המידע לרבות:

1. תשתיות ומערכות חומרה, רכיבי תקשורת ואבטחת מידע;
2. מערכות התוכנה המשמשות את הפעלת מאגר המידע, לניהול המאגר ותחזוקתו, לתמיכה בפעילותו ולאבטחתו;
3. תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר וממנו;
4. תרשים הרשת שפועל בה המאגר, תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה;
5. רשימת מצאי עדכנית.



נוהל אבטחה

בהתאם לסעיף מס' 4 בתקנות הגנת הפרטיות (אבטחת מידע), בעל מאגר המידע נדרש לכתוב "נוהל אבטחת מידע" שכלול בין השאר: הוראות על אבטחה פיזית של אתר המאגר, הרשאות גישה למאגר המידע ולמערכות המאגר, הוראות למורשי הגישה למאגר, פרוט הסיכונים אליהם חשוף המאגר במסגרת פעילותו השוטפת ואופן הטיפול בסיכונים אלו, התמודדות עם אירועי אבטחת מידע לפי חומרת האירוע ולפי רמת רגישות המידע, הוראות ניהול ושימוש התקנים ניידים.

כמו כן במידה ומדובר על מאגר בעל רמת אבטחה בינונית או גבוהה יכללו בנוסף הנהלים הבאים:

1. אמצעי זיהוי ואימות בשביל גישה למאגר ולמערכות המאגר;
2. אופן הבקרה על השימוש במאגר מידע;
3. הוראות על עריכת ביקורות תקופתיות לבדיקת תקינותם של אמצעי האבטחה;
4. הוראות בנוגע לגיבוי נתונים;
5. ביצוע פעולות פיתוח במאגר ואופן הגישה של אנשי הפיתוח למאגר.



ניהול הרשאות כוח אדם

בהתאם לסעיף 8 בתקנות הגנת הפרטיות (אבטחת מידע):

”בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר בהתאם להגדרות תפקיד. הרשאת גישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד”. כמו כן נקבע כי ”בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם ושל בעלי ההרשאות הממלאים תפקידים אלה”



בקרה ותיעוד גישה

בהתאם לסעיף 10 בתקנות הגנת הפרטיות (אבטחת מידע), במערכות מידע של מאגרים בעלי רמת אבטחה בינונית וגבוהה ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הנכנסים למערכת. מנגנון הבקרה יכלול את זהות המשתמש, תאריך ושעת ניסיון הגישה, החלק במערכת שאליו בוצעה הגישה, סוג הגישה, היקפה והאם הגישה אושרה או נדחתה. על בעל המאגר לוודא שאין אפשרות לבטל או לשנות את מנגנון הבקרה וכן לבדוק שהנתונים נשמרים למשך שנתיים לפחות.



אבטחה פיזית

בהתאם לסעיף 6 בתקנות הגנת הפרטיות (אבטחת מידע) על בעל המאגר להבטיח כי המערכות המידע ישמרו במקום מוגן המונע חדירה וכניסה ללא רשות. כמו כן במאגרים ברמת אבטחה בינונית או גבוהה ינקטו באמצעים לבקרה ותיעוד של כניסה ויציאה מהאתרים הפיזיים בהם נמצאות המערכות וכן פיקוח גם על הכנסה והוצאה של ציוד מהאתר ומממנו.

אבטחת תקשורת

בהתאם לסעיף 14 בתקנות הגנת הפרטיות (אבטחת מידע):
"בעל מאגר לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום לנזק או שיבוש למחשב או לחומרים שבמחשב".



התקן נייד

בהתאם לסעיף 12 בתקנות הגנת הפרטיות, על בעל המאגר להגביל או למנוע לחלוטין אפשרות לחיבור התקנים ניידים למערכות המאגר על מנת לשמור על הרמה ההולמת את אבטחת המאגר.

בעל מאגר הבוחר לאפשר שימוש במידע באמצעות התקן נייד, ינקוט בכל אמצעי ההגנה האפשריים על מנת להבטיח את שלמות המידע תוך תשומת לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד.



ביקורות תקופתיות

בהתאם לסעיף 16 בתקנות הגנת הפרטיות, מאגר מידע ברמת אבטחה בינונית או גבוהה מחויב לבצע ביקורת פנימית או חיצונית, על ידי גורם מוסמך לכך שאינו הממונה על אבטחת המאגר, אחת לשנתיים לפחות.

בדוח הביקורת יבדוק המבקר את התאמת אמצעי האבטחה במאגר לנהלים הדרושים ויחפש אחר ליקויים. במידה ומצא, על בעל המאגר לבחון את האפשרות לעדכן את מסמך הגדרות המאמר כך שיתאים למצב החדש ויפעל לתיקון ולשיפור הליקויים.



הגנת הפרטיות –

דוגמאות לאירועים שהתרחשו בשנים האחרונות

דוגמא מס' 1

יולי 2018 – חברת איתוראן

פרטי האירוע:

גורם חיצוני (האקר) פרץ למערכת המידע של החברה וגנב מידע רגיש של מאות אלפי לקוחות בחברה כולל שמות, מספרי ת.ז., פרטי חשבונות בנק, פרטי אשראי, כתובות, מיקום הרכב ועוד... הפריצה תוקנה באופן מהיר יחסית.

פעולות אכיפה:

הרשות להגנת הפרטיות פתחה בהליך אכיפה מנהלי כנגד החברה ומנהליה בטענה של חולשת אבטחה ואי דיווח לרשות.

The screenshot shows a news article on the Galobus website. The article title is "כל הפרטים שלכם חשופים: אירוע אבטחה חמור באתר איתוראן" (All your personal data is exposed: a serious security breach on the Aitoran website). The article text states that a hacker accessed the company's information system, stealing sensitive data of hundreds of thousands of customers, including names, IDs, bank account numbers, credit cards, addresses, and vehicle locations. The breach was quickly fixed. The article is dated 18.07.2018 and is by Alon Lavi-Weinreb. Social media sharing icons for WhatsApp, Facebook, Email, and Print are visible at the bottom of the article.

דוגמא מס' 2

פברואר 2018 – חברת עמותה כנגד הפלות

פרטי הארוע :

אחד מסניפי עמותה שפועלת להסברה כנגד הפלות היו בקשר עם עובדות במרפאה אשר מבצעת הפלות בארץ וקיבלו פרטים אישיים ופרטי התקשרות עם נשים וניסו לשכנע אותן לא לבצע הפלה

פעולות אכיפה :

נפתחה חקירה – שימוש בלתי חוקי במידע אישי.

משרד המשפטים
הרשות להגנת הפרטיות 

שירותים ומידע מדיניות ונהלים פרסומים קבלת קהל חדשות מידע משפטי

gov.il < חדשות < משרד המשפטים < הרשות להגנת הפרטיות < פעילות אכיפה < חקירה פלילית של הרשות להגנת הפרטיות: מיד
המתנגדת לכך

חדשות

**חקירה פלילית של הרשות להגנת הפרטיות:
מידע רפואי רגיש אודות נשים שהתכוונו לבצע
הפלה הועבר לידי עמותה המתנגדת לכך**

נושא: פעילות אכיפה

תאריך פרסום: 20.02.2018

לאחרונה הסתיימה חקירה רגישה שניהלה הרשות להגנת הפרטיות אשר במרכז העברת מידע אודות נשים שהתכוונו לבצע הפלה. המידע הועבר לידי עמותה במרכז הארץ, אשר פעלה להניא את הנשים מלבצע את ההפלה, תוך ניצול המידע הרפואי הרגיש שהועבר לידיה ופגיעה חמורה בפרטיותן.

דוגמא מס' 3

דצמבר 2019 – רמי לוי תקשורת

פרטי הארוע :

רמי לוי הינה חברה קמעונאית גדולה במשק הישראלי ולה חברת בת "רמי לוי תקשורת". מספר מנהלים בחרה עשו להם 'נוהג' (מאות מקרים) בהם נכנסו לפרטי השיחות ואיתרו טלפונים כדי לברר מידע על אנשים, חלקם עובדים.

פעולות אכיפה :

נפתחה חקירה, הוגשו כתבי אישום פליליים נגד החברה, מנהל בכיר ומנהל אבטחת מידע.

כתב אישום בכפוף לשימוע נגד בכירים בחברת הסלולר של רמי לוי על פגיעה בפרטיות

"רמי לוי שיווק השקמה תקשורת" קשורה למערכת של פלאפון המתעדת נתוני תקשורת. עפ"י החשד הבכירים ניצלו אותה לרעה כדי לבלוש אחרי "עובדי החברה ושאינם עובדי החברה, בלא ידיעתם, תוך פגיעה קשה בפרטיותם". בין הבכירים, אופיר אטיאס מנהל החברה וחתנו של רמי לוי

עמיר קורץ 29.12.19 11:27

דוגמא מס' 4

דצמבר 2020 – פרשת שירביט

פרטי האירוע :

מערכות המידע של חברת הביטוח ישראלית נפרצה ונגנבו פרטים אישיים של לקוחות (לרבות גניבת גיבויים). הדרישה לכופר כספי נענתה בשלילה והאקרים מאיימים למכור את המידע שברשותם.

פעולות אכיפה :

האירוע עדין חי, החקירה החלה וקיימת מעורבות של מערך הסייבר הלאומי

ההאקרים שפרצו למערכות של שירביט דורשים כופר של מיליון דולר

בהודעה שפרסמו ההאקרים הלילה הופיעה דרישה לתשלום כופר של כ-50 ביטקוין - כמיליון דולר בשער הנוכחי של מטבע הקריפטו; לטענתם, אם דרישותיהם לא יענו תוך 24 שעות מהבוקר, 8 שעות ירושלים, המחיר יתחיל לעלות. בסוף כל 24 שעות של המתנה הם מתכוונים להדליף מאגר של מסמכים - החל מהבוקר, עת פרסמו מקבץ ראשון של כ-300 מסמכים גנובים

דוגמא מס' 5

2018 – פרשת "והדרת"

פרטי האירוע :

עובדת סוציאלית בבית חולים רמב"ם העבירה מידע אודות חולים סיעודיים המאושפזים בבית החולים ואמורים להשתחרר בקרוב לחברת סיעוד אשר התקשרה למשפחות והציע את שירותי הסיעוד שלהם.

פעולות אכיפה :

עובדים נדונו לקנסות כספיים, ועבודות שירות, חברת הסיעוד נקנסה במאות אלפי שקלים

הפרקליטות: עובדים ברמב"ם ובלאומית מכרו מידע רפואי רגיש על מטופלים לחברות סיעוד

בין החשודים עובדת סוציאלית ואח בבית החולים רמב"ם שבחיפה, עובד בקופת חולים לאומית, שתי חברות סיעוד וכן מנהלים וסוכנים בחברות שירותי סיעוד ושירותי טלרפואה בצפון הארץ

תומר גנון 18.06.17 12:24



DORON YONISY

Risk Management | Chief Risk Officer

תודה רבה על ההקשבה

זמן לשאלות.....

ניתן לפנות גם בטלפון:

דורון יוניסי

050-5400988

או בדוא"ל:

doron@audit-int.co.il

חזרה
להתחלה

חזרה
לפעולות

